ESET REMOTE ADMINISTRATOR / ENDPOINT SECURITY / ENDPOINT ANTIVIRUS

Basic Setup Guide

Published January 2013

Contents

Getting started **1**

Software components **1**

Section 1: Purchasing and downloading your software **1**
- 1.1 Username and Password 1
- 1.2 License file 1
- 1.3 Getting your software 1

Section 2: Installation **2**
- 2.1 ESET Remote Administrator Server 2
- 2.2 ESET Remote Administrator Console 2
- 2.3 Additional options 2

Section 3: Setting up the Mirror server **3**
- 3.1 Mirror server setup 3
- 3.2 Testing your Mirror 3
- 3.3 Server Log settings 3

Section 4: Configuring a default policy **4**
- 4.1 Protect setup parameters 4
- 4.2 Disable splash-screen and nonessential notifications 4
- 4.3 Configure clients to update from the Mirror 4

Section 5: Pushing out ESET Endpoint Security / ESET Endpoint Antivirus to your network **5**
- 5.1 Populate the Remote Install tab and run a diagnostic 5
- 5.2 Push installation checklist 5
- 5.3 Creating a package 6
- 5.4 Pushing out the package 7
- 5.5 Configuring network settings —ESET Endpoint Security Only 7
- 5.6 Protecting your Microsoft Windows Server 7

Section 6: Update Mirror Troubleshooting Checklist **8**
- 6.1 Common Issues 8
- 6.2 Client-side checklist 8
- 6.3 Server-side checklist 8
- 6.4 Before submitting a case 10

ESET REMOTE ADMINISTRATOR / ENDPOINT SECURITY / ENDPOINT ANTIVIRUS

Basic Setup Guide

Copyright © 2013 ESET, spol. s r.o.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without written permission from ESET, spol. s r.o.

ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

Getting started

Protecting your business network with **ESET Endpoint Security / Endpoint Antivirus** is a straightforward process—a basic installation can be completed in a single afternoon. This Basic Setup Guide will walk you through obtaining your ESET software, configuring your server computer and mirror, installing the software on client computers and customizing client settings. The **ESET Remote Administrator User Guide** should also be read in its entirety and referred to whenever necessary throughout the installation process.

ESET Endpoint Security / ESET Endpoint Antivirus, the **ESET Remote Administrator Server** and the **ESET Remote Administrator Console** are the components that support your malware defense system: the antivirus software itself, the server pushing it out to your clients and the administration console you use to monitor the system.

Software components

There are three separate components to your ESET product: the ESET Endpoint Security / Endpoint Antivirus software itself, plus the ESET Remote Administrator Console (ERAC) and the ESET Remote Administrator Server (ERAS). The ESET Remote Administrator Console should be installed on the computer(s) you will be using to manage your network. The ESET Remote Administrator Server should be installed on your server computer. Often in small-business installations, the server computer is the same one you use to manage your network.

Section 1: Purchasing and downloading your software

Estimated time: *30 minutes*

The first step toward protecting your network is obtaining the ESET software components mentioned above. If you have not already purchased an ESET product, please visit the link below:

http://eset.com/store

Once you have purchased your ESET product, you will receive an email from ESET containing your **Username** and **Password** in the body of the email and your **license file** as an attachment to the email.

1.1 Username and Password

Your ESET Username and Password are slightly different than many usernames and passwords with which you may be familiar. They are not user-configured keys that protect your information. They are authentication keys that allow your computer to download your ESET endpoint product and authenticate your ESET endpoint product to update its virus signature database to protect your network from evolving threats. Your ESET Username and Password are automatically generated and cannot be customized.

You will be prompted for your Username and Password several times during initial setup of ESET server / endpoint products. Enter them carefully. Both are case sensitive and the hyphen in the Username is required. Your Password is 10 characters long (all lowercase); if you choose to copy and paste your Username and Password from the license email, be sure to delete any extra empty spaces, which might be interpreted as characters. Your Password will never contain an"L", it's a numeral one (1). A large"O" is the numeral zero. A small"o" is the lowercase letter"o".

Username and Password examples:
Username: EAV-12345678
Pasword: 1a2bc3defg

1.2 License file

Your license file—the attachment called *nod32.lic* or *nod32.zip*—is a file that the ESET Remote Administrator needs to manage your network of protected client computers. It contains authentication for the number of seats (protected computers) and tells ESET Remote Administrator that you are entitled to protect and manage a set number of computers, depending on the bundle you purchased. Save the license file to your Desktop.

1.3 Getting your software

Visit the ESET Download Center using the link below to obtain the components you will need to set up your secure network:

http://www.eset.com/download/business

If you are downloading from the US—Click **I have a license** next to ESET Endpoint Security or ESET Endpoint Antivirus. At the next page select your operating system, bit-architecture and language using the drop-down menus and then click **Download**. See the KB connection on page 2 at the right for help determining which version of ESET Endpoint Security / ESET Endpoint Antivirus is right for your system. Enter your Username and Password and then save the file to your Desktop.

KB connection

Check the ESET Knowledgebase for more info:

What do I do with my ESET security product license files?:

http://kb.eset.com/esetkb/SOLN2253

KB connection

Check the ESET Knowledgebase for more info:

How do I remove an old license file and update ESET Remote Administrator with a new one?

http://kb.eset.com/esetkb/SOLN540

Next, return to **http://www.eset.com/download/business/** and click **Remote Management** to access the ESET Remote Administrator Console and ESET Remote Administrator Server downloads. Click **Download** and then specify your operating system and language to download ESET Remote Administrator Console. Repeat these steps to download ESET Remote Administrator Server. You will be prompted for your Username and Password. Save the files to your Desktop.

Users outside the US—Click **For Business → Remote Management** and download both ESET Remote Administrator Server and ESET Remote Administrator Console. Next click the **Endpoint Security** tab and then click **Download** next to ESET Endpoint Security / ESET Endpoint Antivirus. Save the files to your desktop.

Once your download is complete, we recommend also downloading the ESET Endpoint Security / ESET Endpoint Antivirus installer for the alternative bit-architecture (32-bit if you downloaded 64-bit or vice versa) to simplify push installations to groups of client workstations with both 32 and 64-bit operating systems.

KB connection

Check the ESET Knowledgebase for more info:

Which version (32-bit or 64-bit) of ESET endpoint products should I download? (5.x)

http://kb.eset.com/esetkb/SOLN3013

Section 2: Installation

Estimated time: *15 minutes*

Once you are finished downloading components, you are ready to install. Sections 2.1 through 2.3 assume you are using 32-bit installers. For 64-bit computers, the file names will be slightly different.

IMPORTANT: Install the ESET Remote Administrator Server *on the server that will be managing your network*. This computer *may* be the terminal you are using, but it could also be a headless server in a server rack or offsite. Contact your network administrator if you're unsure.

2.1 ESET Remote Administrator Server

First, double-click the installer .msi for ESET Remote Administrator Server (*era_server_nt32_enu.msi*).

At the **Welcome** screen click **Next**, agree to the **End-User License Agreement** and click **Next**. Under **Select Components**, leave both check boxes selected. **Typical** installation is selected by default, click **Next** again and you will be prompted to browse to your *nod32.lic* file (which you saved to your Desktop in step 1.2).

You are given the option to define security settings for ESET server / endpoint solutions on your network. Since we're keeping it simple here, we recommend you set just one, **Password for Console (Administrator Access)**. This Password protects access to ESET Remote Administrator from unauthorized users. Click **Set** and choose a robust Password you can remember and don't share it. You can go back and add additional security passwords later if you wish. Click **Next**.

Last, enter your ESET-issued Username and Password (as mentioned in Section 1.1) carefully and click **Next**. You can also copy and paste your Username and Password directly from the license email. Click **Next** and then click **Install**.

After installation, the ESET Remote Administrator Server service starts automatically.

2.2 ESET Remote Administrator Console

When the ESET Remote Administrator Server installation wizard process is completed, double-click the ESET Remote Administrator Console installer (*era_console_nt32_enu.msi*). Install the ESET Remote Administrator Console on the computer you plan to use to manage your network. This will likely be the local computer you are using to run the installation wizard. Leave **Typical** installation selected and advance through the options by clicking **Next** until you can click **Install.** The installation progress bar will appear.

2.3 Additional options

Because this is an ESET Remote Administrator Basic Setup Guide, we're skipping over a number of customizable options you may wish to explore at a later time.

For additional information about installations on Microsoft SQL, MySQL or Oracle servers, or for a detailed list of which TCP ports must be open for ESET Remote Administrator to work properly, please see **Section 2** of the **ESET Remote Administrator Manual**.

ESET Remote Administrator Manual

Check the ESET Remote Administrator manual for more info:

2.1.3 Ports used

2.2 Basic installation guide

Section 3:
Setting up the Mirror server

Estimated time: *15 minutes*

Your ESET-protected client workstations get regular updates to the virus signature database from ESET servers. This keeps them current and protected from evolving threats. Having all your clients connect to the ESET servers independently would result in an unnecessary amount of traffic across your local area network (LAN).

ESET Remote Administrator provides a Mirror server (a server that "mirrors" the content available on ESET servers) on your own LAN. This way your clients only need to check locally for new virus signature updates and program component updates.

3.1 Mirror server setup

Open the ESET Remote Administrator Console by clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**. Verify that you are connected to the ESET Remote Administrator Server (**File → Connect**).

In this guide, we're going to use the default Mirror server configuration using internal HTTP. There are other options available, including using a local folder to store update content, as well as instructions for creating replicated Mirror servers for different LANs. See the KB connection at the right for more information.

Click **Tools → Server Options**. Click the **Updates** tab and enter your ESET-issued Username and Password in the **Update Username** and **Update Password** fields in the **Server Options** window (Figure 1-1, at right). Click **Set Password...**to enter your Password.

Select the **Create update mirror** check box in the middle of the window. Select the **Provide update files via internal HTTP** server check box.

Click the **Update now** button to display a confirmation dialog box ('This will first apply server options and then fire the event. Continue?') and click **Yes**.

A dialog box will appear that says "Event fired on the server." This message means that your Mirror successfully checked for and downloaded update content from the ESET servers. Once you see the message "Finished", with the update version number, date and time displayed in the center of the **Update** module, click **OK**.

KB connection

Check the ESET Knowledgebase for more info:

How do I install ESET Remote Administrator and configure a Mirror server? (5.x)

http://kb.eset.com/esetkb/SOLN2993

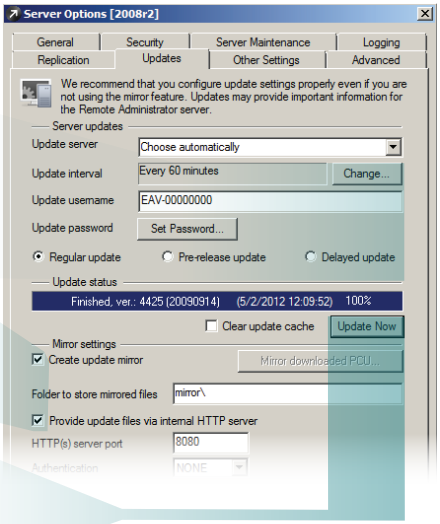

Figure 1-1: The Server Options window

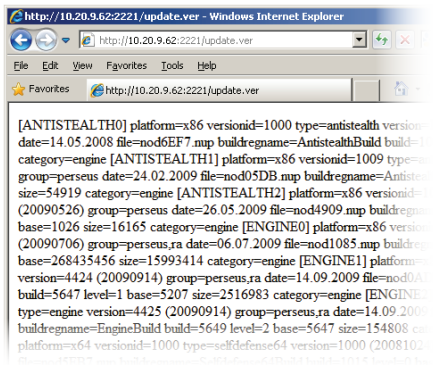

Figure 2-1: Windows Explorer page displaying text from a successful Mirror server connection

3.2 Testing your Mirror

Check that the Mirror server you just created is working. Open a web browser on a client workstation (not the Server) and enter the following into the address bar:

http://Testserver:2221/update.ver
(where "Testserver" is the name of your Server computer)

If your Mirror creation was successful, you will see a text file with information about your Mirror (as in Figure 2-1, at right). If it fails, you will get a standard connection failure error.

3.3 Server Log settings

To preserve database size and maximize performance, ESET Remote Administrator does not log HIPS, Device Control, Web Control, Antispam or Greylist activities on client workstations by default.

You can enable logging of these features from the **Server Options** window. To do so, click **Tools → Server Options** and then click the **Server Maintenance** tab. Click **Log Collecting Parameters** and then set the level of logs for each specific feature using the drop-down menus. When you are finished, click **OK**.

KB connection

Check the ESET Knowledgebase for more info:

What method should I choose in ESET Remote Administrator for my clients to download virus signature updates?

http://kb.eset.com/esetkb/SOLN2337

Section 4: Configuring a default policy

Estimated time: 15 minutes

ESET Remote Administrator allows you to customize the way ESET Endpoint Security / ESET Endpoint Antivirus protects your client computers. To do this, you'll need to configure a default policy. Client workstations will inherit this policy when they check in to the ESET Remote Administrator Server.

From the ESET Remote Administrator Console, click **Tools → Policy Manager**.

You'll see a server icon labeled **Server Policy** (*your server's name*). Click it and then click **Edit...** on the far right of the **Policy Manager** window (Figure 3-1, at right). In the example, the server is named *Testserver*.

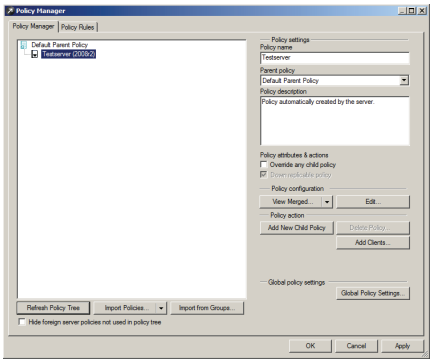

Figure 3-1: Remote Administrator Console > Tools > Policy Manager

This will launch the ESET Configuration Editor–the tool you will use to customize your ESET Endpoint Security / ESET Endpoint Antivirus client settings.

For the purposes of this Basic Setup Guide, we're going to set up a Default Workstation policy, a set of simple configurations that will work on most basic networks with no hassle. If you have highly specific network settings or proprietary software that may need special permissions, check the ESET Remote Administrator Manual for detailed information on building your own custom policy.

4.1 Protect setup parameters

First, we want to make sure your ESET endpoint software cannot be modified by anyone but you or other qualified users. Near the top of the Configuration Editor tree, expand **Windows desktop v5 → Kernel → Settings** and then click **Protect setup parameters**.

When **Protect setup parameters** is highlighted, click **Mark** on the right. Next, double-click **Password to unlock: <Password is not set>**. You will be prompted to choose a password that will be used to allow modifications of your ESET security settings on each of the workstations. We recommend picking a password different from the one from Step 2.1 because you may wish to share one but not the other. Once your password is set, anyone wishing to alter ESET settings on client workstations will be prompted for it.

NOTE: This only affects changes made from the workstations themselves. You can still alter settings remotely from the ERA Console without password authentication.

4.2 Disable splash-screen and nonessential notifications

Now, we want to ensure that your client computers aren't being notified about activities that ESET Endpoint Security / ESET Endpoint Antivirus performs in the background. A little farther down the Configuration Editor tree, expand **Windows desktop v5 → Kernel →Settings → Default user interface values.** Click **Suppress user settings** and then select the **Value: Yes / No** check box.

This will ensure that your settings override any custom settings a user might choose. Next, highlight **Show splash-screen at startup** and on the right, deselect the **Value: Yes / No** check box. Then, highlight **Display only notifications requiring user intervention** and on the right, select the **Value: Yes / No** check box. This ensures that your users' computers will not be disrupted by unnecessary messages from their antivirus software.

ESET Remote Administrator Manual

Check the ESET Remote Administrator manual for more info:

5.3 Policies

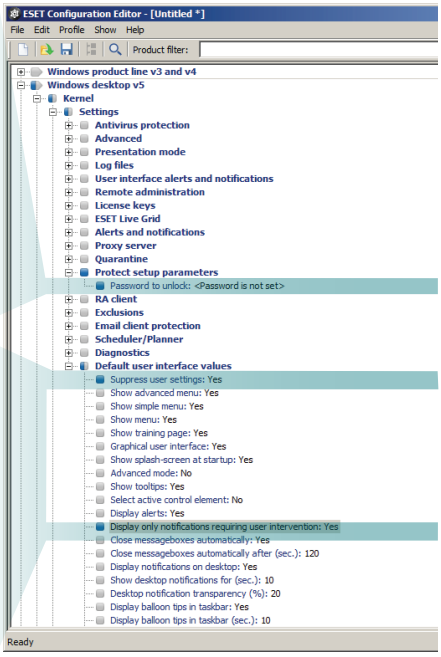

Figure 4-1: Remote Administrator Console > Tools > Policy Manager > Configuration Editor

4.3 Configure clients to update from the Mirror

Next, scroll down the Configuration Editor tree and expand **Update → Profile (My profile) → Settings** and click **Update server: Choose automatically**. Here, we want to configure your clients to update from the Mirror we set up in step 3.1. With **Update server** highlighted, click **Mark** and then on the right, select **<Custom update server>** from the **Value** drop-down menu. Enter the HTTP address of your Mirror in the **Value** field. This will look something like:

http://Testserver: 2221
(Where "Testserver" is your server computer and port 2221 is the default port. Be sure there are no spaces between the server name, the colon [":"] and the port number.)

Click the diskette icon to the save the configuration and then click **Console** to exit the Configuration Editor.

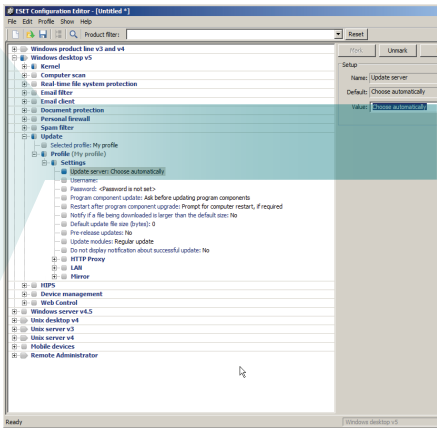

Figure 4-2: Remote Administrator Console > Tools > Policy Manager > Configuration Editor

Section 5: Pushing out ESET Endpoint Security / ESET Endpoint Antivirus to your network

Estimated time: *Varies based on installation checklist, number of seats, prior AV uninstall. Up to one hour.*

Well, you've installed the Console and the Server components of ERA and you've set up the Mirror. You've even built a default policy into your ESET Remote Administrator settings.

The last big step is getting your ESET software out to your client workstations. To do this, ESET Remote Administrator creates a Package (an installer that can be run remotely) and sends one out to each computer on your network so you don't have to walk around from terminal to terminal installing ESET Endpoint Security / ESET Endpoint Antivirus on each one.

Before you create and"push" (send) your package to clients, let's confirm that your network is properly configured for the push installation by populating the **Remote Install** tab and running a diagnostic.

5.1 Populate the Remote Install tab and run a diagnostic

This process will enable ESET Remote Administrator to identify client workstations that can be targeted for a push install.

Click the **Remote Install** tab at the bottom right of the ESET Remote Administrator Console. Select the **Computers** pane, click the **Default Search Task** in the **Search Tasks** window and then click **Run**. Computers from the **Clients** tab will appear in the **Computers** pane. See the KB connection at the right for instructions to create a custom Search Task to filter your results.

Hold **CTRL** and click to select each of the clients to which you will be push installing. Once you are done, right-click a selected client and in the context menu click **Diagnostics of Windows Push Installation**.

In the **Computers Logon Settings** window you can set the domain logon information for each computer. Select your client computer(s) from the list and click **Set** or **Set All** based on whether you need to specify logon information for each computer or all at once. Enter the logon information in the **Logon Information** window, click **OK** and then click **Next**. Click **Finish** to run the diagnostic.

To view the results of your diagnostic, click the **Install Tasks** pane. If no conflicts are detected, the **State** will display as"Finished" once the task is complete. Proceed to Section 5.3 of this guide to create your push install package if your diagnostic finished successfully. If you see the message"Finished With Warning" continue to Section 5.2 to resolve any issues before carrying out your remote installation.

5.2 Push installation checklist

The following checklist details some of the most common issues that can cause a remote installation to fail and how to resolve these issues.

This guide assumes that client workstations on your network all use the same or similar configurations. Therefore, the configuration checklist below only needs to be fulfilled on a single client machine because all other clients should look the same.

For a complete description of the requirements for configuration of a push install, see the KB connection at the right.

- First – and perhaps most important – you need to ensure that any prior antivirus software is uninstalled across your entire network. Running two antivirus products can cause your system to be unstable and can interfere with crucial operations your ESET product needs to perform to protect your network. Follow the KB connection at the right for more information and a list of common uninstaller utilities.
- All workstations on which you are trying to install ESET Endpoint Security / ESET Endpoint Antivirus must answer a ping from the computer where ERA Server is installed.
- Confirm that **Use simple file sharing (Recommended)** is disabled on any Windows XP or Vista workstations and any Windows Server 2000, 2003 or 2008 servers in your network.

KB connection

Check the ESET Knowledgebase for more info:

How do I view specific types or groups of client workstations in the ESET Remote Administrator Console? (5.x)

http://kb.eset.com/esetkb/SOLN3020

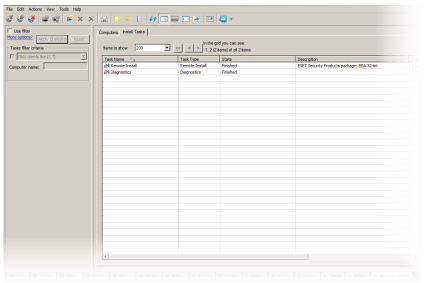

Figure 5-1: The Install Tasks pane

KB connection

Check the ESET Knowledgebase for more info:

ESET Remote Administrator Push Installation Requirements and Checklist

http://kb.eset.com/esetkb/SOLN82

KB connection

Check the ESET Knowledgebase for more info:

Uninstallers (removal tools) for common antivirus software

http://kb.eset.com/esetkb/SOLN146

- For Windows Vista, Windows 7 and Windows Server 2008 operating systems, verify the following:
    - The ESET Remote Administrator service should be run with Domain Administrator permissions.
    - To set Domain Admin. permissions for ESET Remote Administrator, navigate to **Start → Control Panel → Administrative Tools → Services**. Right-click the **ESET Remote Administrator Server** service and then click **Properties** from the context menu.
    - Click the **Log On** tab and then select the radio button next to **This account**. Enter your Domain name and Admin account name in the **This account** field (for example: *MyDomain\AdministratorAccountName*) and then enter your Admin password in the **Password** and **Confirm Password** fields.
- Verify that the workstation(s) can access IPC by issuing the following command from the Command Prompt on the workstation:

    net use \\servername\IPC$

    Where *servername* is the name of the server running ESET Remote Administrator.
- Make sure the client workstation(s) on which you are installing ESET Endpoint Security / ESET Endpoint Antivirus have the shared resource **ADMIN$** activated. Confirm this by clicking **Start → Control Panel → Admin Tools → Computer Mgmnt → Shared Folders → Shares**.
- The user performing the remote installation must have administrative rights and may not have a blank password.
- From the computer where you have ESET Remote Administrator Server installed, verify that you can remotely log on to client workstations.
- Ports 2221-2224 must allow ESET Remote Administrator to communicate. If the server has any of these ports blocked, communication with the workstations is not possible.
- For Windows Vista computers, User Account Control (UAC) should be disabled.
- On client workstations running Windows, the Remote Registry service must be running.

KB connection

Check the ESET Knowledgebase for more info:

Which ports does ESET Remote Administrator use?

http://kb.eset.com/esetkb/SOLN2221

5.3 Creating a package

Once you've verified that your client network is ready to install ESET Endpoint Security / ESET Endpoint Antivirus, you will need to create a package installation from the ESET Remote Administrator Console. Open it by clicking **Start → All Programs → ESET → ESET Remote Administrator Console**. At the bottom of the ERAC window, click the **Remote Install** tab and then click **Actions → Manage Packages...**.

To add an installation package, click **Add...** in the **Installation Packages Editor** window.

Click **Download From The Web** and browse for the ESET Endpoint Security / ESET Endpoint Antivirus installation file and then click **Create** to download the installer file and create the installation package.

Click **Save As** and give your installation package a descriptive name, such as"ESET Endpoint Security Install". Click **Save** and then click **Close** to return to the ERAC window.

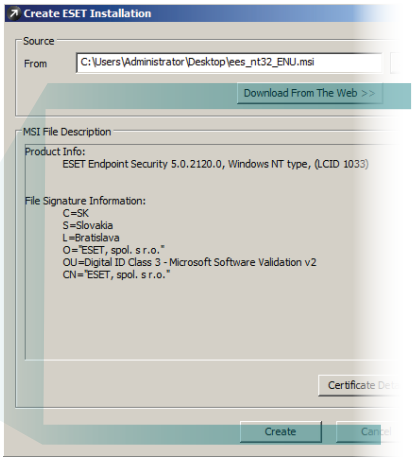

Figure 6-1: the Package Creation window

5.4 Pushing out the package

Now that the installation package is ready, choose the client computers from the ERAC and send it out. To do so, click the ESET Remote Administrator Console **Remote Install** tab hold **CTRL** and then click to select each of the clients to which you would like to push out the installation package. Right-click the selected clients and click **Windows Push Installation**. This may also be accomplished by clicking **Actions** and then clicking **Windows Push Installation**.

In the **Computers Logon Settings** window, you can set the domain logon information for each computer. Select the computer(s) from the list and click **Set** or **Set All**, based on whether you need to specify logon information for each computer or all at once. Enter the logon information in the **Logon Information** window, click **OK** and then click **Next**.

In the **Package Settings** window, select **ESET Security Products package** from the **Type** drop-down menu. Select your saved installation package ("ESET Endpoint Security Install" from step 5.2) from the **Name** drop-down menu.

Name your Remote Install task and set the time you'd like it performed (immediately or on a specific date and time) in the **Task Settings** window. Click **Finish** to apply your Remote Install task.

After you have completed the installation process, click the **Clients** tab at the bottom of the ERAC window and wait for your client computers to check in. When all of the computers to which you pushed ESET Endpoint Security / ESET Endpoint Antivirus appear in the right-hand area, your push installation is complete.

NOTE: *Clients will take about ten minutes to log in after the completion of your initial push install. Some clients may report an update failure immediately after installation. This is because they have not yet received the policy created in Section 4. This will automatically be resolved within an hour.*

5.5 Configuring network settings—ESET Endpoint Security Only

Congratulations, you have successfully completed your push installation!

If you installed ESET Endpoint Antivirus on all client workstations, no further adjustments are needed. For clients on which you installed ESET Endpoint Security, take the following steps to ensure stable communications between your clients and server.

A **New network connection detected** dialog box will appear the first time that ESET Endpoint Security is run. Click **Allow sharing** to keep ESET Endpoint Security from detecting ESET Remote Administrator as a potential threat and blocking communications to the ESET Remote Administrator server.

The default setting for the Personal firewall in ESET Endpoint Security is **Automatic mode**. We recommend leaving client workstations that will remain on your office network at all times in **Automatic mode** to avoid connectivity issues.

For client workstations that will be used on third-party or public networks, see the **ESET Endpoint Security User Guide** for more information on configuring the Personal firewall. To download the user guide, please visit the link below:

http://download.eset.com/manuals/eset_ees_userguide_enu.pdf

5.6 Protecting your Microsoft Windows Server

If your Windows server will be used for browsing the internet and / or processing email and will therefore be exposed to security risks, we recommend that you install ESET File Security for Microsoft Windows Server.

ESET File Security for Windows Server is optimized to protect server-based file systems without causing the types of conflicts that can occur from installing an endpoint-based file-protection solution on a server. For more information on ESET File Security for Microsoft Windows Server, see the KB connection at the right.

KB connection

Check the ESET Knowledgebase for more info:

How do I push install to client(s) using ESET Remote Administrator? (5.x)
http://kb.eset.com/esetkb/SOLN2982

How do I push uninstall to client workstations using ESET Remote Administrator? (5.x)
http://kb.eset.com/esetkb/SOLN2991

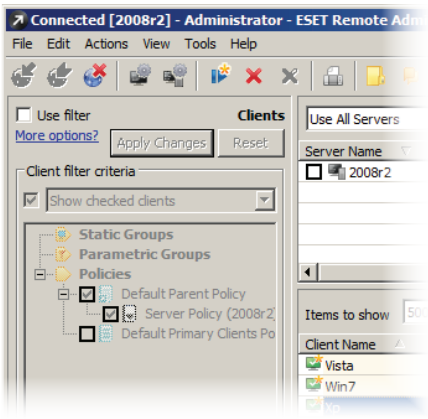

Figure 7-1: Select your client computers from the Computers tab on the right. Right click them and click Windows Push Installation

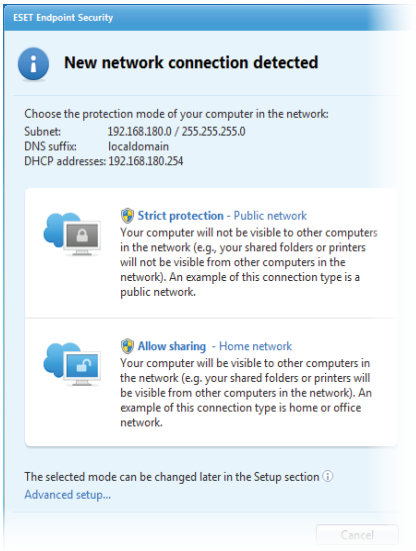
ESET Endpoint Security
New network connection detected
Choose the protection mode of your computer in the network:
Subnet: 192.168.180.0 / 255.255.255.0
DNS suffix: localdomain
DHCP addresses: 192.168.180.254
Strict protection - Public network
Your computer will not be visible to other computers in the network (e.g., your shared folders or printers will not be visible from other computers in the network). An example of this connection type is a public network.
Allow sharing - Home network
Your computer will be visible to other computers in the network (e.g. your shared folders or printers will be visible from other computers in the network). An example of this connection type is home or office network.
The selected mode can be changed later in the Setup section
Advanced setup...
Cancel

Figure 8-1: The New network connection detected dialog

KB connection

Check the ESET Knowledgebase for more info:

ESET File Security for Microsoft Windows Server FAQ

http://kb.eset.com/esetkb/SOLN2789

Section 6: Update Mirror Troubleshooting Checklist

This is a comprehensive checklist for troubleshooting issues with the ESET Remote Administrator Server Mirror. In many cases, completing the items in this checklist will resolve your update issues.

6.1 Common Issues

- Update fails or finishes with a warning
- AUTHORIZATION_FAILED(0x2001) error
- Client workstations are unable to retrieve updates from the ESET Remote Administrator Server Mirror
- A conflict exists between the ESET RA HTTP Server service and the ESET HTTP Server service

6.2 Client-side checklist

- Clear the update cache and try to update again
- Verify that the client workstation is able to reach the mirror (*http://servername:2221/update.ver*):

  1. Configure an ESET client workstation to access the Mirror server in ESET Remote Administrator (5.x)

  2. If the Mirror still cannot be reached, verify that the Windows firewall on the server, or any other firewalls, is allowing TCP traffic on port 2221

  3. Test connectivity from the workstation computer to the server using Telnet:

     telnet SERVERNAME:2221

  NOTE: *If Telnet is not installed, you can install it from an administrative command prompt with the following command:*

     pkgmgr /iu:"TelnetClient"

6.3 Server-side checklist

- Verify that server update settings are configured properly in the ESET Remote Administrator Console:

  1. Set up a Mirror server in ESET Remote Administrator

  2. Clear the update cache and try to update again

- Verify that the Windows firewall is allowing TCP traffic on port 2221:

  1. Click **Start** » **Administrative Tools** » **Windows Firewall with Advanced Security**.

  2. Click Inbound **Rules** » **New Rule**.

  The same Windows Firewall exception should be added for Outbound Rules as well.

  3. Select **Port** and click **Next**.

  4. Select **TCP** » Specific local ports and then enter **2221-2224** into the blank field. Click **Next**.

  5. Select **Allow the connection** and click **Next**.

  6. Deselect the check box next to **Public** and click **Next**.

  7. Type a name for the rule into the **Name** field and click **Finish**.

- Delete the mirror folder from the file system and let the ESET Remote Administrator Server recreate it by performing an update:

  1. Make sure that **Show hidden files, folders, and drives** is enabled:

KB connection

Check the ESET Knowledgebase for more info:

Error downloading file and cannot update virus signature database (5.x)

http://kb.eset.com/esetkb/SOLN2875

KB connection

Check the ESET Knowledgebase for more info:

How do I install ESET Remote Administrator and configure a Mirror server? (5.x)

http://kb.eset.com/esetkb/SOLN2993

Why is the ESET Remote Administrator Server not updating to the most recent virus signature database?

http://kb.eset.com/esetkb/SOLN2220

a. Click **Start** » **Control Panel** » **Folder Options**.

b. Click the **View** tab, select **Show hidden files, folders, and drives** and then click c. Click the **View** tab, select **Show hidden files, folders, and drives** and then click **OK**.

2. Navigate to the **Mirror** folder, right-click it and select **Delete**. Click **Yes** to confirm.

NOTE: *The location of this folder will vary depending on operating system and Mirror configuration.*

Server 2008R2: C:*ProgramData**ESET**ESET Remote Administrator**Server**Mirror*

XP/Server 2003: C:*Documents and Settings**All Users**Application Data**ESET**ESET Remote Administrator* *Server**mirror*

3. Open the ESET Remote Administrator Console and click **Tools** » **Server Options**.

4. Click the **Updates** tab, select the check box next to **Clear update cache** and then click **Update Now**. When prompted to fire the event, click **Yes**.

- Verify that the ESET RA HTTP Server service is set to manual and logged in as the Network Service account:

  1. Click **Start**, type services.msc into the search field and press **Enter**.

  2. Locate the ESET RA HTTP Server service in the **Name** column.

  3. Verify that **Manual** is listed in the Startup Type column.

  4. Verify that Network Service is listed in the Log On As column.

- Verify that the http Mirror service is running and or can be restarted successfully If not:

  a. *Verify that the client on the server is not also attempting to host the mirror*

  b. *Verify that there are not any other services listening on the mirror (port 2221 by default)*

You can use Telnet (http://windows.microsoft.com/en-US/windows-vista/Telnet-commands) or NetStat (http://technet.microsoft.com/en-us/library/bb490947.aspx) to complete this step.

- Verify that the mirror folder exists in the file system:

  1. Make sure that Show hidden files, folders, and drives is enabled:

  a. Click **Start** » **Control Panel** » **Folder Options**.

  b. Click the **View** tab, select **Show hidden files, folders, and drives** and click **OK**.

  2. Navigate to the Mirror folder. The location of this folder will vary depending on operating system and Mirror configuration.

  Server 2008R2: C:*ProgramData**ESET**ESET Remote Administrator**Server**Mirror*

  XP/Server 2003: C:*Documents and Settings**All Users**Application Data**ESET**ESET Remote Administrator**Server**mirror*

- Verify the path of the mirror. If a non-standard location is set then set it to the default of, Mirror\

  1. Open the ESET Remote Administrator Console and click **Tools** » **ESET Configuration Editor**.

  2. Expand **Remote Administrator** » **ERA Server** » **Settings** » **Mirror** and select Mirror folder.

  3. If you see a path other than *mirror*\ in the Value field, highlight it and

KB connection

Check the ESET Knowledgebase for more info:

How do I restart the ESET Remote Administrator Server service?

http://kb.eset.com/esetkb/SOLN743

replace it with *mirror*\(the default folder).

4. Save your changes and exit the ESET Configuration Editor.

5. Click **Tools** » **Server Options**, click the **Update** tab, and then click **Update Now**.

- Verify that the mirror folder is up to date:
  1. Make sure that **Show hidden files, folders, and drives** is enabled:
     a. Click **Start** » **Control Panel** » **Folder Options**.
     b. Click the **View** tab, select Show hidden files, folders, and drives and click **OK**.
  2. Navigate to the Mirror folder in your file system, double-click it and then open the *update.ver* file in notepad.
  3. Search the file for today's date in European format (for example, 20121108). The virus signature database version will be displayed next to the date, which you can compare to the latest version of the virus signature database (http://go.eset.com/us/threat-center/threatsense-updates/).

- Delete the contents of the Windows Temp folder and/or check the permissions.
  1. Navigate to C:\Windows\Temp
  2. Verify that the user has"Full Control" by right-clicking the Temp folder and clicking **Properties** » **Security** tab.
  3. Once you have verified that the user has Full Control access, delete the contents of the Temp folder.

6.4 Before submitting a case

If you are still experiencing issues and are going to submit a case, you can expedite our response time by having a SysInspector log and .xml configuration ready:

I. Create a SysInspector log by following the steps below:

1. Download ESET SysInspector (http://www.eset.com/us/download/utilities/).

2. Click Download next to your desired version. When prompted to **Run** or **Save**, click **Save** and save the file to your Desktop.

3. Double-click the SysInspector icon on your Desktop and click **Run**.

4. Click I Agree. Once the analysis is finished, the ESET SysInspector main program window will open.

5. Click **File** » **Save Log**. Click **Yes** to confirm and then save the log file to your Desktop.

NOTE: *Before you save the log file, make sure that ESET SysInspector Compressed Log (*.zip) is selected from the Save as type drop-down menu.*

6. Please attach this log to your email reply to ESET Customer Care. We will examine the log and respond as soon as possible with the recommended action based on our findings.

II. Export an .xml configuration.

III. Please attach this log to your email reply to ESET Customer Care. We will examine the log and respond as soon as possible with the recommended action based on our findings.

KB connection

Check the ESET Knowledgebase for more info:

How do I export a configuration to an .xml file to help ESET Customer Care resolve my issue? (Business Users)

http://kb.eset.com/esetkb/SOLN2691

Thank you for choosing ESET!

ESET North America, 610 West Ash Street, Suite 1700, San Diego, CA 92101 U.S.A.
Toll Free: +1 (866) 343-3738 | Tel. +1 (619) 876-5400 | Fax. +1 (619) 876-5845

www.eset.com

© 1999-2012 ESET, LLC d/b/a ESET North America. All rights reserved. ESET, the ESET Logo, ESET SMART SECURITY, ESET CYBERSECURITY, ESET.COM, ESET.EU, NOD32, INSTALL CONFIDENCE, SAFE MADE SAFER, SECURING OUR ECITY, VIRUS RADAR, THREATSENSE, SYSINSPECTOR, THREAT RADAR, and LIVE GRID are trademarks, service marks and/or registered trademarks of ESET, LLC d/b/a ESET North America and/or ESET, spol. s r.o. in the United States and certain other jurisdictions. All other trademarks and service marks that appear in these pages are the property of their respective owners and are used solely to refer to those companies' goods and services.